



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,315	03/10/2004	Daniel ManHung Wong	OR03-15501	1742
51967 7590 06/18/2008 PVE -- ORACLE INTERNATIONAL CORPORATION c/o PARK, VAUGHAN & FLEMING LLP 2820 FIFTH STREET DAVIS, CA 95618-7759				
			EXAMINER RAAB, CHRISTOPHER J	
			ART UNIT 2166	PAPER NUMBER
			MAIL DATE 06/18/2008	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/800,315

**Applicant(s)**

WONG, DANIEL MANHUNG

**Examiner**

Christopher J. Raab

**Art Unit**

2166

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 29 February 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,3-5,7,8,10-12,14,15,17-19 and 21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3-5,7,8,10-12,14,15,17-19 and 21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

01. This action is in response to Applicant's amendment filed on **02/29/08**. **Claims 1, 3 – 5, 7 – 8, 10 – 12, 14 – 15, 17 – 19, and 21** are pending in the present application. **This action is made FINAL**, as necessitated by amendment.

#### ***Claim Rejections – 35 USC § 112***

02. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention

03. **Claims 3 – 5, 7, 10 – 12, 14, 17 – 19, and 21** recite the limitation “the mismatch alert”. There is insufficient antecedent basis for this limitation in the claim. It is believed that the limitation “the mismatch alert” was intended to read as “the SQL injection” and has been treated as such for the remainder of this Office Action. Appropriate correction is required.

#### ***Claim Rejections - 35 USC § 103***

04. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2166

05. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

06. **Claims 1, 3 – 5, 7 – 8, 10 – 12, 14 – 15, 17 – 19, and 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chaudhuri et al. (US Patent 7,194,451)**, hereinafter 'Chaudhuri', in view of **Sin Yeung Lee, "Learning Fingerprints for a Database Intrusion Detection System"**, 2002 (as supplied by the IDS filed on September 01, 2005), hereinafter "Lee".

Consider **claim 1**, Chaudhuri discloses a method for using query signatures in a database, comprising:

probing query type objects, so as to create signatures for queries, such that the query signatures are determined based on the structure of the query and not based on the values of the parameter values (read as trapping database queries in a controlled environment, parsing the database queries to produce a set of valid signatures, wherein parsing the database queries involves determining signatures for the queries, wherein the signature [comprises] SQL keywords contained in the corresponding query with literals removed) (column 4 line 52 – column 5 line 28);

monitoring a system that receives queries (read as receiving a query at the database) (column 2 lines 26 – 54);

generating a query signature, which is defined as a query with the same structure, but different constants, and that that SQL can be used for the queries (read as parsing the query at the database to determine a signature for the query, wherein the signature comprises SQL keywords contained in the corresponding query with literals removed) (column 2 lines 46 – 54, column 7 line 40 – column 8 line 2, column 1 lines 31 – 38).

comparing query signatures to see if it matches an acceptable query (read as determining if the signature is located in the signature cache, which contains signatures for valid queries) (column 7 line 40 – column 8 line 2);

However, Chaudhuri does not specifically disclose that the query signatures are used to detect intrusion, by way of (SQL) injection.

In the same field of endeavor, Lee discloses a method such that query statements are matches with a set of fingerprints of legitimate signatures, and will disallow any SQL query that does not match (read as identifying the query as being SQL injected and rejecting the query) (page 268, section 3, lines 5 - 18).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the SQL intrusion detection taught by Lee into the query signature creation method taught by Chaudhuri for the purpose of preventing harmful SQL injection attempts of the database.

Consider **claim 3**, and **as applied to claim 1 above**, Lee discloses a method such that anomalies or intrusions are interpreted as errors and are channeled to the

reaction module (read as the mismatch alert throws an error) (page 268, section 3, lines 5 - 18).

Consider **claim 4**, and **as applied to claim 1 above**, Lee discloses a method such that an administrator can be alerted when such an intrusion attempt occurs (read as the mismatch alert is sent to a database administrator and the query is processed)

Consider **claim 5**, and **as applied to claim 1 above**, Lee discloses a method such that output can be returned to the user (read as the mismatch alert is sent to a requesting application, thereby allowing the requesting application to take action) (page 268, section 3, lines 5 - 18).

Consider **claim 7**, and **as applied to claim 1 above**, Chaudhuri discloses a method such that a valid query can be added to the signature cache (read as if the signature generates a mismatch alert and if the query is a valid query, the method further comprises allowing a database administrator to add the signature to the signature cache) (column 10 lines 56 – 67).

Consider **claim 8**, Chaudhuri discloses a computer-readable storage medium for using query signatures in a database, comprising:

probing query type objects, so as to create signatures for queries, such that the query signatures are determined based on the structure of the query and not based on the values of the parameter values (read as trapping database queries in a controlled environment, parsing the database queries to produce a set of valid signatures, wherein parsing the database queries involves determining signatures for the queries, wherein the signature comprises SQL keywords contained in the corresponding query with

literals removed, and storing the valid signatures in the signature cache) (column 4 line 52 – column 5 line 28);

monitoring a system that receives queries (read as receiving a query at the database) (column 2 lines 26 – 54);

generating a query signature, which is defined as a query with the same structure, but different constants, and that SQL can be used for the queries (read as parsing the query at the database to determine a signature for the query, wherein the signature comprises SQL keywords contained in the corresponding query with literals removed) (column 2 lines 46 – 54, column 7 line 40 – column 8 line 2, column 1 lines 31 – 38);

comparing query signatures to see if it matches an acceptable query (read as determining if the signature is located in the signature cache, which contains signatures for valid queries) (column 7 line 40 – column 8 line 2);

However, Chaudhuri does not specifically disclose that the query signatures are used to detect intrusion, by way of (SQL) injection.

In the same field of endeavor, Lee discloses a method such that query statements are matches with a set of fingerprints of legitimate signatures, and will disallow any SQL query that does not match (read as identifying the query as being SQL injected and rejecting the query) (page 268, section 3, lines 5 - 18).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the SQL intrusion detection taught by Lee

into the query signature creation method taught by Chaudhuri for the purpose of preventing harmful SQL injection attempts of the database.

Consider **claim 10**, and **as applied to claim 8 above**, Lee discloses a method such that anomalies or intrusions are interpreted as errors and are channeled to the reaction module (read as the mismatch alert throws an error) (page 268, section 3, lines 5 - 18).

Consider **claim 11**, and **as applied to claim 8 above**, Lee discloses a method such that an administrator can be alerted when such an intrusion attempt occurs (read as the mismatch alert is sent to a database administrator and the query is processed)

Consider **claim 12**, and **as applied to claim 8 above**, Lee discloses a method such that output can be returned to the user (read as the mismatch alert is sent to a requesting application, thereby allowing the requesting application to take action) (page 268, section 3, lines 5 - 18).

Consider **claim 14**, and **as applied to claim 8 above**, Chaudhuri discloses a computer-readable storage medium such that a valid query can be added to the signature cache (read as if the signature generates a mismatch alert and if the query is a valid query, the method further comprises allowing a database administrator to add the signature to the signature cache) (column 10 lines 56 – 67).

Consider **claim 15**, Chaudhuri discloses an apparatus for using query signatures in a database, comprising:

probing query type objects, so as to create signatures for queries, such that the query signatures are determined based on the structure of the query and not based on



the values of the parameter values (read as trapping database queries in a controlled environment, parsing the database queries to produce a set of valid signatures, wherein parsing the database queries involves determining signatures for the queries, wherein the signature comprises SQL keywords contained in the corresponding query with literals removed) (column 4 line 52 – column 5 line 28);

monitoring a system that receives queries (read as receiving a query at the database) (column 2 lines 26 – 54);

generating a query signature, which is defined as a query with the same structure, but different constants, and that SQL can be used for the queries (read as parsing the query at the database to determine a signature for the query, wherein the signature comprises SQL keywords contained in the corresponding query with literals removed) (column 2 lines 46 – 54, column 7 line 40 – column 8 line 2, column 1 lines 31 – 38);

comparing query signatures to see if it matches an acceptable query (read as determining if the signature is located in the signature cache, which contains signatures for valid queries) (column 7 line 40 – column 8 line 2);

However, Chaudhuri does not specifically disclose that the query signatures are used to detect intrusion, by way of (SQL) injection.

In the same field of endeavor, Lee discloses a method such that query statements are matches with a set of fingerprints of legitimate signatures, and will disallow any SQL query that does not match (read as identifying the query as being SQL injected and rejecting the query) (page 268, section 3, lines 5 - 18).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the SQL intrusion detection taught by Lee into the query signature creation method taught by Chaudhuri for the purpose of preventing harmful SQL injection attempts of the database.

Consider **claim 17**, and **as applied to claim 15 above**, Lee discloses a method such that anomalies or intrusions are interpreted as errors and are channeled to the reaction module (read as the mismatch alert throws an error) (page 268, section 3, lines 5 - 18).

Consider **claim 18**, and **as applied to claim 15 above**, Lee discloses a method such that an administrator can be alerted when such an intrusion attempt occurs (read as the mismatch alert is sent to a database administrator and the query is processed)

Consider **claim 19**, and **as applied to claim 15 above**, Lee discloses a method such that output can be returned to the user (read as the mismatch alert is sent to a requesting application, thereby allowing the requesting application to take action) (page 268, section 3, lines 5 - 18).

Consider **claim 21**, and **as applied to claim 15 above**, Chaudhuri discloses a apparatus such that a valid query can be added to the signature cache (read as if the signature generates a mismatch alert and if the query is a valid query, the method further comprises allowing a database administrator to add the signature to the signature cache) (column 10 lines 56 – 67).

***Response to Arguments***

07. Applicant's arguments with respect to claims 1, 3 – 5, 7 – 8, 10 – 12, 14 – 15, 17 – 19, and 20 have been considered, but are moot in view of the new ground(s) of rejection.

Applicant argues that Chaudhuri does not disclose the capability to "differentiate SQL keywords from SQL literals". Examiner respectfully disagrees. Chaudhuri disclose, among other things, the capability to use signatures, for query access. In fact, one embodiment creating a signature, is storing all parts of a query except for their parameters (constants). This is exactly what the Applicant appears to be claiming, in that the functionality of the query is the focus of attention, and the mere literals do not have an impact on determining whether the query is the same to another query or valid query signature. The Applicant further argues that Chaudhuri teaches assigning an integer value to the query, and that no other information relating to the query is extracted or stored. Examiner agrees that one embodiment of Chaudhuri does teach this, but however is not limited to such teachings. In fact, Chaudhuri discloses four kinds of signatures, logical query signatures, physical plan signatures, logical transaction signatures, and physical transaction signatures. It is a presumptuous conclusion to assume that Chaudhuri teaches no capability to read a query based on its operations.

In any event, a new reference has been added to help disclose portions of the Applicant's claimed invention. Lee discloses the usage of fingerprints to prevent SQL injection. In fact, Lee goes into detail about the problems of SQL injection, and

discusses several ways to help prevent it and ways to deal with it after it has occurred. Examiner agrees that, as argued by Applicant, that Chaudhuri deals more with database performance, and does not go into great detail about intrusion detection. However, as per the rejections above, Lee has been used to disclose most of this. Therefore, the combination of Chaudhuri's teachings with Lee's teaching, disclose all limitations of the claims.

### ***Conclusion***

08. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

09. Any response to this Office Action should be **faxed to (571) 273-8300 or mailed to:**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Hand-delivered responses** should be brought to

Customer Service Window  
Randolph Building  
401 Dulany Street  
Alexandria, VA 22314

10. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Christopher Raab whose telephone number is (571) 270-1090. The Examiner can normally be reached on Monday-Friday from 8:30am to 6:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Hosain Alam can be reached on (571) 272-3978. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you

Art Unit: 2166

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Christopher Raab  
C.R./cr

June 10, 2008

/K. B. P./

/Hosain T Alam/

Supervisory Patent Examiner, Art Unit 2166